instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form, and to decrypt the encrypted code in electronic form based on a public key of the first party to generate decrypted selected elements[[,]]; and

proving, by the decrypted selected elements, the transaction, ~~wherein the decrypted selected elements are used by the second party to prove the transaction.~~

4. (Currently Amended) A method of verifying a transaction conducted between a first party and a second party, the method comprising:

receiving transaction elements of the transaction;

identifying at least a portion of the received transaction elements as selected elements;

attaching at least a portion of the received transaction elements to a certificate template;

encrypting the selected elements based on a private key of the first party to generate an encrypted code;

attaching the encrypted code to the certificate template to produce a transaction certificate;

transmitting the transaction certificate with the encrypted code to the second party; ~~and~~

instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate decrypted selected elements[[,]]; and

proving, by the decrypted selected elements, the transaction, ~~wherein the decrypted selected elements are used by the second party to prove the transaction.~~

9. (Currently Amended) A method of verifying a transaction conducted between a first party and a second party, the method comprising:

receiving transaction elements of the transaction;

identifying at least a portion of the received transaction elements as selected elements;

attaching at least a portion of the received transaction elements to a certificate template;

encrypting the selected elements based on a private key of the first party to generate an encrypted code;

attaching the encrypted code to the certificate template to produce a transaction certificate;

retrieving a public key of the second party;

encrypting the transaction certificate based on the retrieved public key of the second party, to generate an encrypted transaction certificate;

transmitting the encrypted transaction certificate to the second party;

instructing the second party to decrypt the transmitted encrypted transaction certificate based on a private key of the second party, to produce a decrypted transaction certificate that includes the encrypted code; ~~and~~

instructing the second party to decrypt the included encrypted code based on a public key of the first party to generate decrypted selected elements[[,]]; and

proving, by the decrypted selected elements, the transaction. ~~wherein the decrypted selected elements are used by the second party to prove the transaction.~~

14 (Currently Amended) A method of verifying a transaction conducted between a first party and a second party, the method ~~by the second party~~ comprising:

identifying, by the second party, a portion of transaction elements of the transaction;

transmitting, by the second party, transaction elements of the transaction and the identification of the transaction elements to the first party;

receiving, by the second party, a hard copy transaction certificate that includes an encrypted code;

scanning, by the second party, the received transaction certificate to convert the encrypted code to electronic form;

retrieving, by the second party, a public key of the first party; and

decrypting, by the second party, the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements,

wherein the decrypted proof elements are used by the second party to prove the transaction.

15. (Currently Amended) A method of verifying a transaction conducted between a first party and a second party, the method comprising:

transmitting transaction elements of the transaction to the first party;

receiving a transaction certificate that includes an encrypted code;

retrieving a public key of the first party; ~~and~~

decrypting by the second party the included encrypted code based on the retrieved public key of the first party to generate decrypted proof elements[[,]];and

proving, by the generated decrypted proof elements, the transaction. ~~wherein the decrypted proof elements are used to prove the transaction.~~

16. (Currently Amended) A method of verifying a transaction conducted between a first party and a second party, the method comprising:

making a public key of the second party available to the first party;

transmitting transaction elements of the transaction to the first party;

receiving an encrypted transaction certificate;

decrypting the received encrypted transaction certificate based on a private key of the second party so as to generate a transaction certificate with an encrypted code;

retrieving a public key of the first party; ~~and~~

decrypting, by the second party, the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements[[,]]; and

using the decrypted proof elements ~~are used~~ to prove the transaction.

17. (Currently Amended) A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving, by a third party, a hard copy transaction certificate with an encrypted code ~~by a third party~~;

scanning the received transaction certificate to convert the encrypted code into electronic form;

retrieving a public key of the first party;

decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

declaring the transaction between a first party and a second party including the decrypted proof elements as authenticated by the third party if the decrypting is successful.

18. (Previously Presented) A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving, by a third party, a transaction certificate with an encrypted code;

retrieving a public key of the first party;

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

declaring the transaction between a first party and a second party including the decrypted proof elements as authenticated if the decrypting is successful.

19. (Original) A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving, by a third party, an encrypted transaction certificate;

decrypting the received encrypted transaction certificate based on a private key of the third party so as to generate a transaction certificate with an encrypted code;

retrieving a public key of the first party;

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

declaring the transaction including the decrypted proof elements as authenticated if the decrypting is successful.

20. (Previously Presented) A computing device for verifying a transaction conducted between a first party and a second party, the device comprising:

a receiving module configured to receive transaction elements of the transaction from the second party;

an attachment module configured to attach at least a portion of the received transaction elements to a certificate template;

a first encryption module configured to identify at least a portion of the received transaction elements as selected elements, to encrypt the selected elements based on a private key of the first party to generate an encrypted code, and to attach the encrypted code to the certificate template to produce a transaction certificate; and

a transmission module configured to transmit the transaction certificate from the first party to the second party,

wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction.

21. (Previously Presented) A computing device for verifying a transaction conducted between a first party and a second party, the device comprising:

a receiving module configured to receive transaction elements of the transaction from the second party;

a first encryption module configured to identify at least a portion of the received transaction elements as selected elements, to encrypt the selected elements based on a private key of the first party to generate an encrypted code, and to attach the encrypted code and at least a portion of the received transaction elements to a transaction certificate;

a second encryption module configured to encrypt the transaction certificate based on a public key of the second party to generate an encrypted transaction certificate; and

a transmission module configured to transmit the encrypted transaction certificate from the first party to the second party,

wherein the encrypted transaction certificate is decrypted by the second party based on a private key of the second party to generate a decrypted transaction certificate with the encrypted code, wherein the encrypted code is decrypted based on a public key of the first party to generate decrypted selected elements, and wherein the decrypted selected elements are used by the second party to prove the transaction.

22. (Currently Amended) A computing device for verifying a transaction conducted between a first party and a second party, the device comprising:

a submitting module configured to submit transaction elements of the transaction from the second party to the first party;

a receiving module configured to receive a transaction certificate including an encrypted code from the first party to the second party; and

a first decryption module configured to decrypt the encrypted code to generate decrypted proof elements, based on a public key of the first party,

wherein the second party proves the transaction with the decrypted proof elements ~~are used to prove the transaction~~.

23. (Currently Amended) A computing device for verifying a transaction conducted between a first party and a second party, the device comprising:

a submitting module configured to submit transaction elements of the transaction from the second party to the first party;

a receiving module configured to receive an encrypted transaction certificate from the first party to the second party;

a first decryption module configured to decrypt the received encrypted transaction certificate, based on a private key of the second party, to generate an decrypted transaction certificate with an encrypted code; and

a second decryption module configured to decrypt the encrypted code based on a public key of the first party to generate decrypted proof elements,

wherein the second party proves the transaction with the decrypted proof elements ~~are used to prove the transaction.~~

2497555
040406